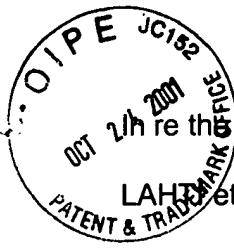


PATENT APPLICATION #3

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE



Where the Application of:

LAHTI et al.

Application No.: 09/939,717

Group Art Unit: 2131

Filed: August 28, 2001

Attorney Dkt. No.: 108347-00009

For: SOFTWARE VIRUS PROTECTION

RECEIVED  
OCT 26 2001  
Technology Center 2100

CLAIM FOR PRIORITY

Commissioner for Patents  
Washington, D.C. 20231

October 24, 2001

Sir:

The benefit of the filing dates of the following prior foreign application in the following foreign country is hereby requested for the above-identified patent application and the priority provided in 35 U.S.C. §119 is hereby claimed:

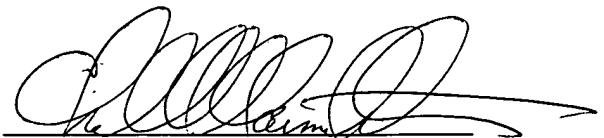
British Patent Application No. 0021281.1 filed on August 31, 2000

In support of this claim, certified copy of said original foreign application is filed herewith.

It is requested that the file of this application be marked to indicate that the requirements of 35 U.S.C. §119 have been fulfilled and that the Patent and Trademark Office kindly acknowledge receipt of these/this document.

Please charge any fee deficiency or credit any overpayment with respect to this paper to Deposit Account No. 01-2300.

Respectfully submitted,

  
Douglas H. Goldhush  
Registration No. 33,125 *Key No. 25,895*

Customer No. 004372  
AREN'T FOX KINTNER PLOTKIN & KAHN, PLLC  
1050 Connecticut Avenue, N.W.,  
Suite 400  
Washington, D.C. 20036-5339  
Tel: (202) 857-6000  
Fax: (202) 638-4810  
DHG:baw

**This Page Blank (uspto)**



**CERTIFIED COPY OF  
PRIORITY DOCUMENT**

PATENTS • DESIGNS  
The  
Patent  
Office  
COPYRIGHT • TRADE MARKS



INVESTOR IN PEOPLE

The Patent Office  
Concept House  
Cardiff Road  
Newport  
South Wales  
NP10 8QQ



RECEIVED  
OCT 26 2001  
Technology Center 2100

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

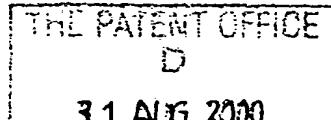
In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.

Signed

Dated 19 September 2001

This Page Blank (uspto)



## Request for grant of a patent

(See the notes on the back of this form. You can also get an explanatory leaflet from the Patent Office to help you fill in this form)

31 AUG 2000 E364606-11 D01063  
P01/77000 0.00-0021281.1

31 AUG 2000

The Patent Office

Cardiff Road  
Newport  
South Wales  
NP10 8QQ

## 1. Your reference

RL.P51227GB

0021281.1

2. Patent application number  
(The Patent Office will fill in this part)

F-Secure Oyj  
Pyynttie 7  
PL24  
FIN-02231  
Espoo  
Finland  
FINLAND

Patents ADP number (if you know it)

7807167001

If the applicant is a corporate body, give the country/state of its incorporation

## 4. Title of the invention

SOFTWARE VIRUS PROTECTION

## 5. Name of your agent (if you have one)

Marks &amp; Clerk

"Address for service" in the United Kingdom to which all correspondence should be sent (including the postcode)

Marks & Clerk  
4220 Nash Court  
Oxford Business Park South  
Oxford  
OX4 2RU

Patents ADP number (if you know it)

727 1125 001

## 6. If you are declaring priority from one or more earlier patent applications, give the country and the date of filing of the or of each of these earlier applications and (if you know it) the or each application number

Country

Priority application number  
(if you know it)Date of filing  
(day / month / year)

## 7. If this application is divided or otherwise derived from an earlier UK application, give the number and the filing date of the earlier application

Number of earlier application

Date of filing  
(day / month / year)

## 8. Is a statement of inventorship and of right to grant of a patent required in support of this request? (Answer 'Yes' if:

Yes

- a) any applicant named in part 3 is not an inventor, or
- b) there is an inventor who is not named as an applicant, or
- c) any named applicant is a corporate body.

See note (d))

9. Enter the number of sheets for any of the following items you are filing with this form.  
Do not count copies of the same document

Continuation sheets of this form	(none)
Description	6
Claim(s)	2
Abstract	1
Drawing(s)	2 ✓

10. If you are also filing any of the following, state how many against each item.

Priority documents	(none)
Translations of priority documents	(none)
Statement of inventorship and right to grant of a patent (Patents Form 7/77)	
Request for preliminary examination and search (Patents Form 9/77)	1 /
Request for substantive examination (Patents Form 10/77)	1 /
Any other documents (please specify)	(none)

11.

I/We request the grant of a patent on the basis of this application.

Signature Marks & Clerk Date

Marks & Clerk

30 August, 2000

12. Name and daytime telephone number of person to contact in the United Kingdom

Dr. Robert Lind 01865 397900

#### Warning

After an application for a patent has been filed, the Comptroller of the Patent Office will consider whether publication or communication of the invention should be prohibited or restricted under Section 22 of the Patents Act 1977. You will be informed if it is necessary to prohibit or restrict your invention in this way. Furthermore, if you live in the United Kingdom, Section 23 of the Patents Act 1977 stops you from applying for a patent abroad without first getting written permission from the Patent Office unless an application has been filed at least 6 weeks beforehand in the United Kingdom for a patent for the same invention and either no direction prohibiting publication or communication has been given, or any such direction has been revoked.

#### Notes

- If you need help to fill in this form or you have any questions, please contact the Patent Office on 0645 500505.
- Write your answers in capital letters using black ink or you may type them.
- If there is not enough space for all the relevant details on any part of this form, please continue on a separate sheet of paper and write "see continuation sheet" in the relevant part(s). Any continuation sheet should be attached to this form.
- If you have answered 'Yes' Patents Form 7/77 will need to be filed.
- Once you have filled in the form you must remember to sign and date it.
- For details of the fee and ways to pay please contact the Patent Office.

DUPLICATE

## Software Virus Protection

The present invention relates to software virus protection, and in particular to virus protection for wireless devices.

5

Viruses are a serious problem to users of computers. In order to combat the problem, there are a variety of anti-virus software products available which are able to identify viruses resident in the files or memory of a computer. Modern anti-virus software, such as for example F-Secure Anti-Virus for Windows NT, uses a virus signature comparison in order to identify viruses. Each virus contains code which can be analysed and recorded on a database. The database need not record all of the code contained in a virus if a unique "digital fingerprint" or signature can be recorded instead. This may be for example the overall pattern of the code, or two or three particular lines. When a signature comparison is made, the anti-virus program searches for viruses by scanning a file for the presence of a virus signature such as are present in the database.

Clearly, if effective protection is to be maintained, the database used by the anti-virus software must contain signatures for all known viruses. Unfortunately, new viruses are detected all the time, currently at the rate of one per day. Once a newly detected virus has been analysed by the anti-virus software provider and a signature created, the database must be updated on all of the computers which are using the anti-virus software. There have been various methods up until now for carrying out this update.

25 The earliest method used by virus software providers was to send a diskette through the mail to registered users of the anti-virus software, this diskette containing the required updates to the database. Another method has been to make the virus updates available on-line, so that they can be obtained by connecting to a remote server maintained by the anti-virus software provider. Updates have also been provided in the form of 30 attachments to e-mail.

Increasingly, mobile phones are being used to connect to the Internet. Mobile Internet access is being facilitated by new networks (incorporating HSCSD and GPRS) as well

as other protocols such as WAP. As mobile "platforms" with wireless modems and internet connections become more powerful, Internet connections will be as easy to obtain as for a desktop PC. This increase in the usage and capacity of mobile platforms renders them susceptible to attack by viruses. The methods outlined above for updating 5 anti-virus software can also be used for mobile platforms. However, in general they will not be permanently connected to the Internet, and indeed may only connect to the Internet occasionally. This can lead to the signature database used by anti-virus software becoming out of date, rendering protection incomplete. Out of date protection can be worse than no protection at all, as it can engender a false sense of security in a 10 user.

It is, therefore, an object of the present invention to provide a means for updating anti-virus signature databases on mobile platforms.

15 According to a first aspect, the present invention provides a method of updating a virus signature database used by anti-virus software operating on a mobile wireless platform, the method comprising sending update data via a signalling channel of a mobile telecommunications network to the mobile wireless platform.

20 The update data sent to the mobile wireless platform may be a virus signature database update, or may be a software update such as a software patch.

Preferably, the network is a GSM based network or an evolved GSM network such as 25 GSM phase 2 (including GPRS) or UMTS (3GPP).

30 Preferably, the update data is obtained in one or more Short Message Service (SMS) messages. The SMS protocol, as set out for example in the ETSI GSM 03.40 specification, is a protocol which is well known and widely used for data transfer between mobile devices. For example, programs executing on top of the EPOC operating system have access to SMS communications.

Alternatively, the update data may be carried by one or more Unstructured Supplementary Services Data (USSD) messages.

In order to prevent the update information from attack, the payload of the message carrying the update data is preferably cryptographically signed.

5 The mobile platform may be a mobile telephone, communicator, PDA, palmtop or laptop computer, or any other suitable platform.

10 The mobile platform may send a report to a management centre following the successful receipt and installation of the update data. More preferably, this is returned to a management centre using an SMS message.

15 In a preferred embodiment, the present invention provides a method of protecting a wireless device against viruses, comprising maintaining a database of virus signatures on the device, updating the database by receiving data containing virus signatures in one or more Short Message Service (SMS) or Unstructured Supplementary Services Data (USSD) messages, and searching for viruses contained in the database.

Some preferred embodiments of the invention will now be described by way of example only and with reference to the accompanying drawings, in which:

20 Figure 1 is a schematic diagram showing a system according to a preferred embodiment of the invention; and

Figure 2 is a flow diagram of a method of protecting a mobile device from attack by viruses according to a preferred embodiment of the present invention.

25 Figure 1 illustrates a UMTS Mobile Network comprising a UMTS Terrestrial Radio Access Network (UTRAN) consisting of Base Stations (BS) 1 and Radio Network Controllers (RNCs) 2, and a core network consisting of MSCs (and SGSNs) 3 and a transmission network 4 (RNCs of the UTRAN may be supplemented with BSCs to facilitate interworking with the GSM standard). Also present in the core network are a 30 Short Message Service (SMS) centre 5 and a GPRS Gateway Support Node (GGSN) 6. For the sake of simplicity, Figure 1 shows only a single RNC 2 and MSC (SGSN) 3. It will be appreciated that further nodes will be present in a UMTS network in practice.

A mobile wireless device 7 can connect to other telecommunication devices (e.g. mobile telephones, fixed line telephones, etc) via the UTRAN and the core network (of course other networks including "foreign" mobile networks and PSTN networks may be involved in such connections). Using the GGSN 6, the device 7 is able to connect to the  
5 Internet 8. A user of the mobile wireless device 1 may thus contact for example a remote web server 9 by entering the URL of the web server into his device's Internet browser. The mobile device 1 may also communicate with a bluetooth device 10 and a Local Area Network (LAN) 11. By way of example, the mobile device 1 may use the EPOC™ operating system.

10

In view of the risk that viruses could be downloaded from another mobile device, from the remote server 9 via the Internet 8, from the bluetooth device 10, or from another node of the LAN 11, the device 1 is provided with an anti-virus software application which may check any files downloaded from an external source, together with files  
15 already resident on the device's system. As explained above, this software searches files for virus "signatures" so that, in order to be fully effective, it requires its database of virus signatures to be updated regularly.

There are various known methods for obtaining updates to a database of virus  
20 signatures. One method is to periodically receive media (e.g. floppy disks, compact discs) with the updates recorded thereon. However, this is a cumbersome and expensive method and will result in fewer updates being made, with the database never being fully up to date. A better method is for the user of the mobile device to contact a remote web server operated by the provider of the anti-virus software. The necessary data to update  
25 the anti-virus database can then be downloaded from that server. As explained above however, very few mobile devices are permanently connected to the Internet, and in may cases users will only connect to the Internet infrequently. This method also relies on the user remembering to connect to the remote anti-virus server periodically in order to obtain the update data. Thus there will again be periods of time during which the  
30 database is not fully up to date.

In order to overcome these problems use may be made of the SMS centre 5 within the UMTS core network. SMS is a service provided by current GSM networks for sending

short messages over a signalling channel, and is expected to be provided also by UMTS networks.

The SMS centre 5 is located in the core network part of the UMTS network and is 5 coupled to the Internet 8 via an anti-virus server 12 which is operated and controlled by the UMTS network operator. The anti-virus server 12 receives regular updates (e.g. every morning) from an update server 13 maintained by the anti-virus software provider. The SMS server 12 maintains a record of all subscribers to the anti-virus service in a database 13, and initiates virus signature database updates by sending a 10 Short Message Service (SMS) request for each of the registered subscribers (including the user of the mobile device 1) to the SMS centre 5. Upon receipt of a request, the SMS centre 5 generates a corresponding SMS message and send this to the destination mobile device via the Mobile Switching Centre 3 of the core network and the UTRAN. The SMS message contains virus signature data enabling the mobile device 1 to update 15 the anti-virus database to include signatures for those viruses discovered since the last update was made.

As SMS messages can carry only relatively small quantities of information, it may be necessary for the SMS centre 5 to send a "concatenated message", (i.e. several SMS 20 messages) to convey all the necessary information to perform a database update. For the same reason it is desirable to be able to reduce the volume of information sent as part of a virus signature database upgrade. Thus, whilst SMS updates may be sent automatically to all subscribers from the network, it is preferable to send an SMS message to the server 12 from a device 1 (via the SMS centre 5), containing details of 25 which virus signatures are currently stored in the device's signature database. On receipt of such an SMS request, the anti-virus server 12 needs only to issue an SMS request to the SMS centre 5 containing virus signatures not currently on the signature database of the mobile device 1.

30 As noted in the preceding paragraph, SMS updates may be sent automatically from the network to subscribers, or may be triggered by requests from subscribers. Figure 2 is a flow diagram illustrating the sequence of steps involved in a subscriber initiated updating process. The mobile device executes the anti-virus software 21. This is

usually done when the device is switched on. The anti-virus software, which uses a database of virus signatures, checks to determine when the database was last updated 22. If the last update took place more than a pre-defined period ago, e.g. one week, the software causes the device to send an SMS message 23 to the server anti-virus 12 via 5 the SMS centre 5. This message contains data regarding the current status of the database.

In reply to this SMS message, the anti-virus server 12 returns an SMS request 24 (or several SMS messages forming a “concatenated message”) to the SMS centre 5, the 10 request containing signatures for viruses discovered and analysed since the previous update. The SMS centre 5 generates a corresponding SMS message 25 and sends this to the mobile device 1, which receives the message 26 and causes the new signature(s) to be incorporated into the anti-virus signature database for future use 27.

15 When next requested, or otherwise triggered (e.g. by a scanning scheduler), the anti-virus software scans the files and memory of the mobile device in order to determine the presence of any of the virus signatures in its database 28. If an infected file is discovered 29, the user is warned 30 and given an opportunity to delete or clean that file. Otherwise, once all files have been scanned, the software informs the user that his 20 system is “clean” 31.

It will be appreciated that there are other embodiments which fall within the scope of the invention. For example, the method of the present invention may be used to update the anti-virus software itself, e.g. by sending software patches.

**CLAIMS:**

1. A method of updating a virus signature database used by anti-virus software operating on a mobile wireless platform, comprising sending update data via a 5 signalling channel of a mobile telecommunications network to the mobile wireless platform.
2. A method according to claim 1, wherein the update data sent to the mobile wireless platform is a virus signature database update.
- 10 3. A method as claimed in claim 1 or 2, wherein the network is GSM or enhanced GSM network.
4. A method as claimed in claim 3, wherein the update data is carried by one or 15 more Short Message Service (SMS) messages.
5. A method as claimed in claim 1, 2 or 3, wherein the update data is carried by one or more Unstructured Supplementary Services Data (USSD) message.
- 20 6. A method as claimed in any preceding claim, wherein the message carrying the update data is cryptographically signed.
7. A method as claimed in any preceding claim, wherein the mobile platform comprises a mobile telephone, communicator, PDA, palmtop or laptop computer.
- 25 8. A method as claimed in any preceding claim, and comprising sending the update data in response to a request from the mobile platform.
9. A method as claimed in claim 8, wherein said request identifies the current 30 status of a virus signature database.
10. A method of protecting a wireless device against viruses, comprising: maintaining a database of virus signatures on the device;

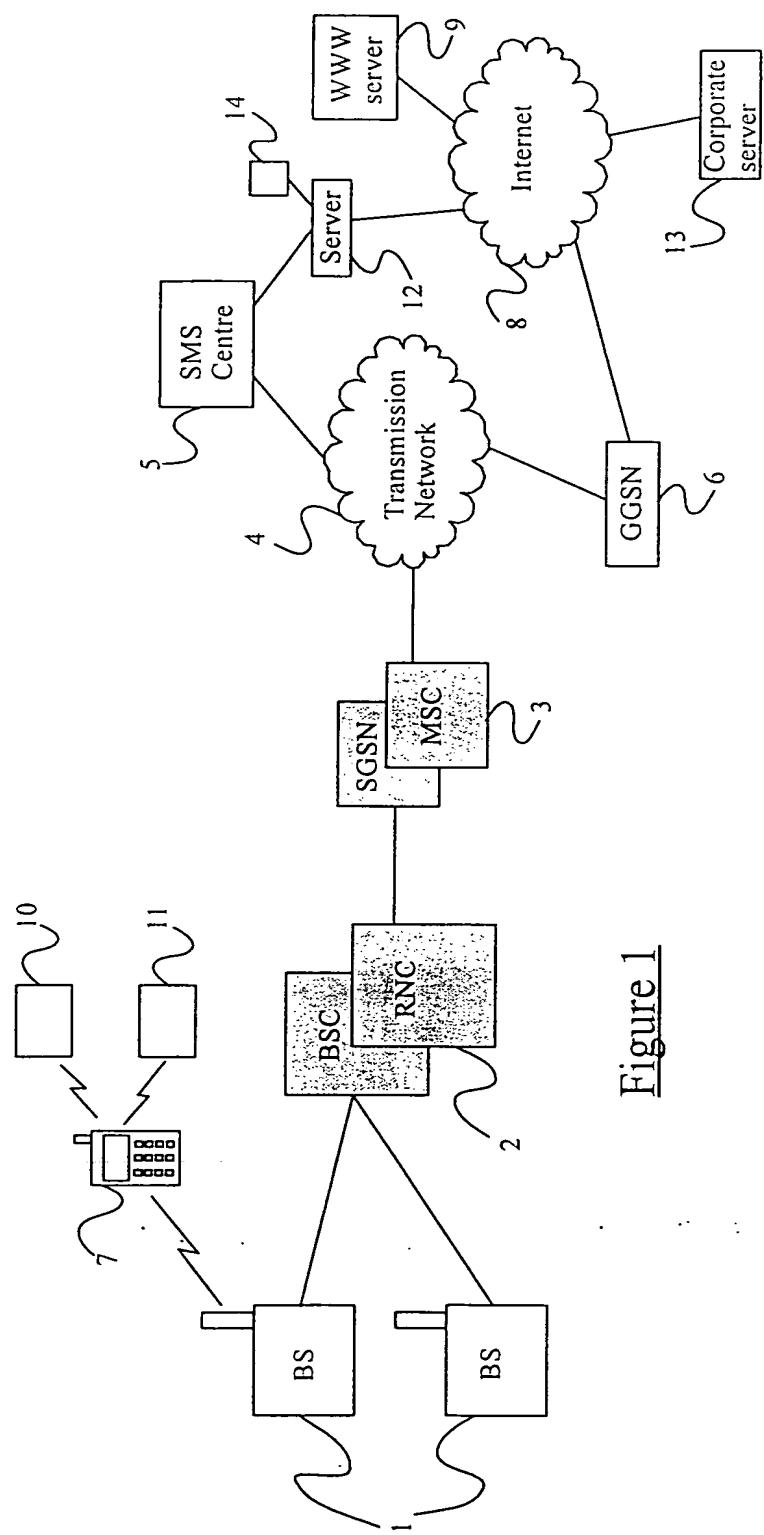
updating the database by receiving data containing virus signatures in one or more Short Message Service (SMS) or Unstructured Supplementary Services Data (USSD) messages; and

searching for virus signatures contained in the database.

**ABSTRACT**  
**Software Virus Protection**

A method of protecting a wireless device against viruses, comprising maintaining a  
5 database of virus signatures on the device, updating the database by downloading virus  
signatures in a Short Message Service (SMS) Message, and searching for virus  
signatures in the memory of or files stored on the wireless device by comparison with  
the database.

10 Figure 2



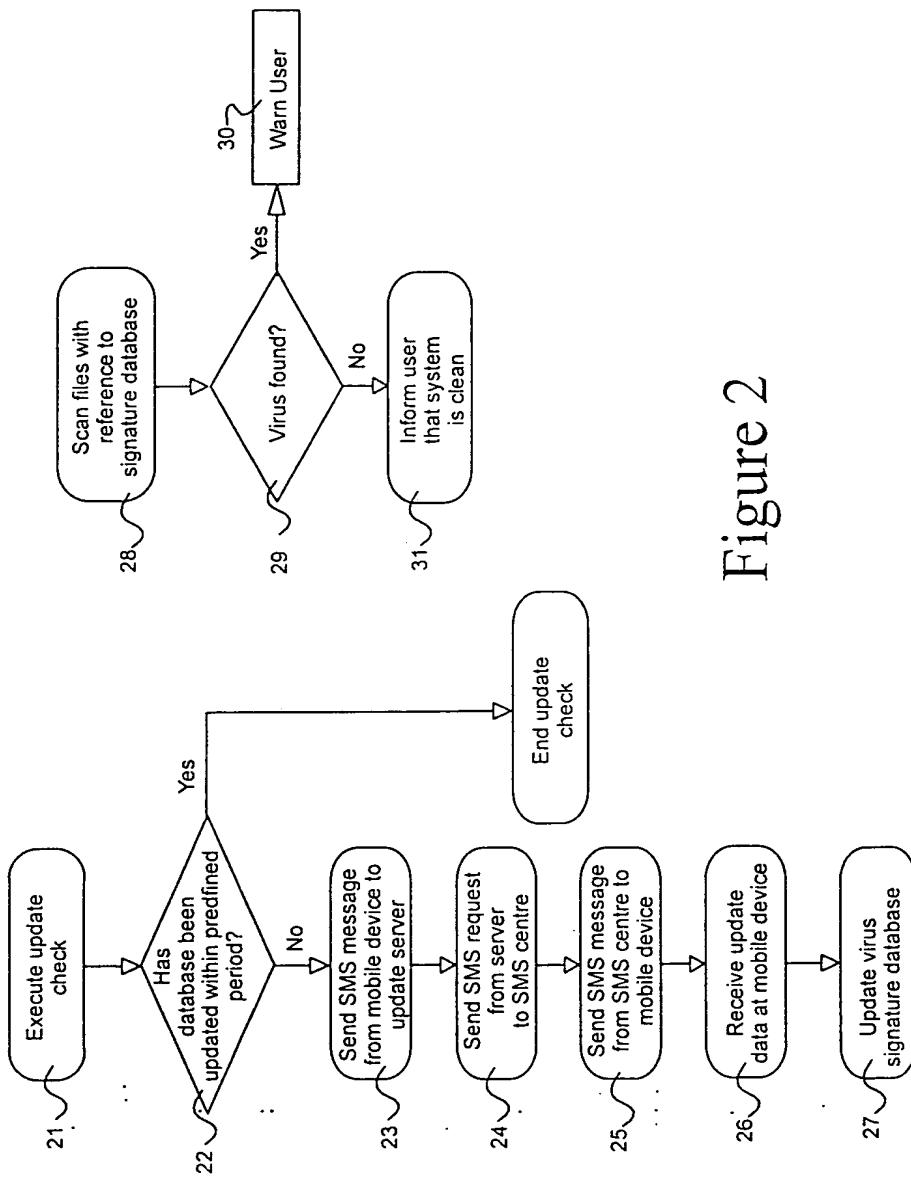


Figure 2

THIS PAGE BLANK (USPTO)

ARENT FOX KINTNER PLOTKIN & KAHN, PLLC  
1050 Connecticut Avenue, N.W., Suite 400  
Washington, D.C. 20036-5339  
Docket No. 108347-00009  
Serial No.: 09/939,717 Filed: August 28, 2001  
Inventor: LAHTI et al.